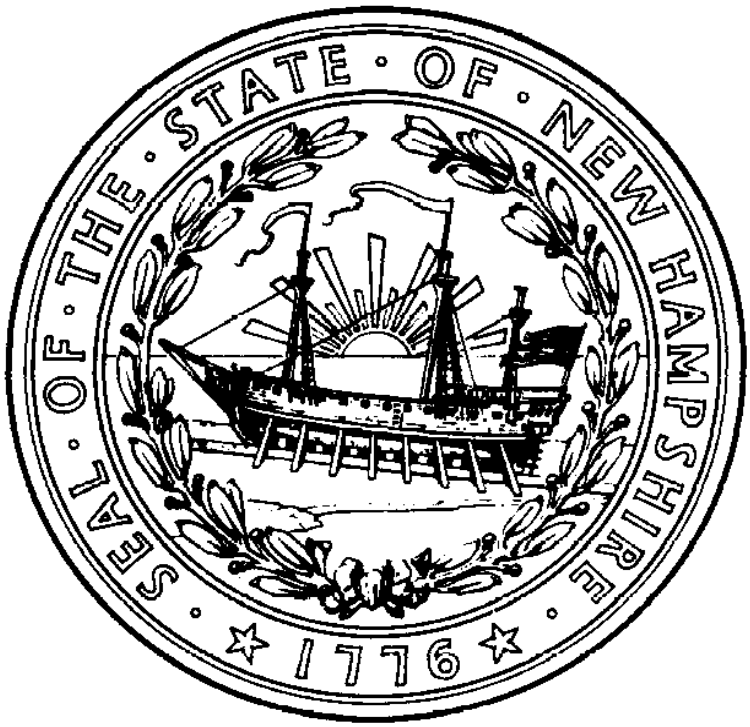
STATE OF NEW HAMPSHIRE

STRATEGIC PLAN TO ADDRESS CYBER CRIME



MAY 2004

State of New Hampshire Strategic Plan to Address Cyber Crime

May 2004

Introduction

Cyber crime, or more broadly, electronic crime, presents ongoing challenges to criminal justice organizations at all levels. Fundamental issues, such as a lack of common vernacular and limited knowledge for quantifying the extent of the problem, hinder strategic efforts by criminal justice agencies to address the challenges posed by this fast-growing crime. A recent white paper by the Joint Council on Information Age Crime reports that, "computer-related crime is costing billions of dollars in damages and losses, and overwhelming law enforcement." Identity theft alone is the fastest growing crime in the country. With no reprieve in sight, many state and local agencies that represent the majority of criminal justice agencies in America lack the resources and training to successfully meet the challenges presented by electronic crimes.

Because of the borderless nature of electronic crimes such as identity theft, child pornography, and cyber attacks, criminal justice agencies must adapt their responses to meet this new threat. The structure and geographic organization of the criminal justice system has had a profound effect on how criminal justice agencies respond to electronic crime challenges. The capability to effectively respond to cyber crime will drive prevention efforts and substantially affect public safety, economic stability, and homeland security in New Hampshire. This Strategic Plan outlines the steps that should be taken by state and local criminal justice agencies in New Hampshire to address cyber crime.

Performance-Based Strategy

The Department of Justice, through the leadership of the Attorney General, together with state and local criminal justice agencies and other stakeholders, have concluded that a statewide performance-based strategy is required to address the unique problems presented by cyber crime. This Strategic Plan outlines a clear mission based upon a consensus of the parties, along with a method for gauging progress, in order to deliver the greatest public safety to the citizens of New Hampshire.

Mission Statement

To develop and maintain an effective statewide response to computer crime and enhance public safety through a collaborative approach between federal, state, and local criminal justice agencies with an emphasis upon comprehensive investigations, forensic evaluations, prosecution, and community outreach activities.

Vision Statement

Our mission will be accomplished through collaborative enforcement efforts, training, acquisition of resources, and enhanced public awareness throughout the State of New Hampshire.

Strategic Objectives

1. To Develop and Deliver Statewide Cyber Crime Investigative Capabilities

Background

- Computers and computer networks are becoming increasingly involved not only in the commission of crimes, but also as a source of valuable information in investigations that are not related to a specific crime (for example, missing persons cases).
- Unlike traditional crimes, cyber crime has no geographical boundaries and therefore requires local, state, and sometimes nationwide cooperation in order to be thoroughly investigated.
- Criminal investigations of cyber crime and related problems require a unique set of skills and technologies.
- The skills required for cyber crime investigations are necessary for ensuring homeland security.
- Only a handful of agencies in New Hampshire have the ability to investigate and prosecute cyber crime. Those that have this ability are limited in the types of crimes that they can investigate.
- The majority of criminal justice in New Hampshire occurs at the local and county level. No single agency in New Hampshire has the resources or expertise to adequately address the scope of problems associated with cyber crime.

Immediate Goals

- 1.1 - To combine and coordinate New Hampshire's resources in order to develop a statewide cyber crime investigative capability by:
    a. Developing a plan for a statewide network that will expand and integrate New Hampshire's investigative capabilities.
    b. Conducting regularly scheduled meetings in order to coordinate statewide criminal justice efforts.
    c. Entering into statewide partnerships with both criminal justice agencies and private entities.

d. Providing information and support to criminal justice agencies on cyber crime problems through the development and distribution of regular memoranda and other materials.

- 1.2 - To train and educate criminal justice agencies in the investigation of cyber crime by:
    a. Identifying and utilizing available resources in order to meet New Hampshire's goals.
    b. Developing statewide standards and protocols to ensure the efficient and consistent investigation of cyber crime.
    c. Providing statewide training to criminal justice agencies at a minimal cost.
    d. Efficiently utilizing state resources by properly identifying and training suitable investigators from criminal justice agencies.
    e. Entering into partnerships with out-of-state entities to increase joint investigative abilities.
- 1.3 - To track New Hampshire's cyber crime investigative capabilities in order to assess its needs on a regular basis by:
    a. Producing regular reports that gauge the progress of New Hampshire's cyber crime investigative capabilities.
    b. Analyzing data from progress reports and interpreting those results to gain an accurate picture of New Hampshire's progress.

2. To Develop and Deliver Statewide Cyber Forensics Capabilities

Background

- Digital evidence, which is available from many new devices, has unique properties that require specialized examiners and tools to reveal and analyze such evidence so that it will stand up to legal scrutiny.
- The need to conduct forensic examinations of computers involved in crimes is growing faster than New Hampshire's criminal justice agencies are able to respond.

Immediate Goals

- 2.1 - To coordinate and increase New Hampshire's cyber crime forensic capability by developing a plan for a statewide cyber forensics network, coordinated by the New Hampshire State Police, which will allow local criminal justice agencies to access advanced technologies that are used to analyze cyber crime by:

a. Identifying the appropriate forensic model for New Hampshire through the study of similar efforts by other states.

b. Identifying and utilizing available forensic resources to meet New Hampshire's needs and projected goals.

c. Developing pilot projects based on existing capabilities.

d. Identifying ways to use additional personnel to compliment criminal justice efforts for cyber forensics.

- 2.2 - To continually increase and streamline New Hampshire's cyber forensic capability and to foster expertise in cyber forensics at the local level by:

    a. Conducting regular training at minimal cost to criminal justice agencies.

    b. Identifying statewide tools and templates for cyber forensics.

    c. Identifying opportunities to acquire equipment by combining purchase orders statewide in order to negotiate lower costs.

    d. Entering into out-of-state partnerships in order to increase New Hampshire's cyber forensic capabilities.

- 2.3 - To accurately track New Hampshire's cyber forensic capabilities in order to assess its needs on a regular basis by:

    a. Producing regular reports that gauge the progress of New Hampshire's cyber forensic capabilities.

    b. Analyzing data from progress reports and interpreting those results to gain an accurate picture of New Hampshire's progress.

3. To Develop and Deliver Statewide Cyber Crime Prosecutorial Capabilities

Background

- Prosecutors must be able to understand the technologies involved in a computer related investigation and must be able to present those technologies in a way that both judges and juries can understand.
- Special attention should be paid to the drafting of search warrants for digital evidence. New digital storage devices and local and state laws may dictate specific criteria.
- Prosecutors must have a thorough understanding of the rapidly growing body of law regarding the prosecution of computer related crimes.

Immediate Goals

- 3.1 - To coordinate efforts to develop statewide cyber crime prosecutorial capabilities and to make the most efficient use of resources through the development of expertise among the county attorneys by:
    a. Identifying and conducting regular training at minimal cost to state, county, and local agencies.
    b. Identifying and utilizing federal resources to meet state, county, and local prosecutorial needs.
- 3.2 - To develop a plan for educating the judiciary on cyber crime issues.
- 3.3 - To track New Hampshire's prosecutorial capabilities accurately in order to assess its needs through regular reporting by:
    a. Producing regular reports that gauge the progress of New Hampshire's cyber prosecutorial capabilities.
    b. Analyzing data from progress reports and interpreting those results to gain an accurate picture of New Hampshire's progress.
- 3.4 - To enter into out-of-state partnerships with other criminal agencies in order to increase New Hampshire's prosecutorial capabilities.

4. To Develop and Deliver Statewide Outreach /Prevention /Preparedness Programs

Background

- Partnerships must be developed between government, businesses, academia, not for profit entities, and the public. This can be accomplished through outreach programs emphasizing the roles these groups have to play in the overall prevention of cyber crime.
- Educational programs targeted at different groups, such as school children (explaining the dangers of the Internet), senior citizens (preventing computer fraud and identity theft), and businesses (computer security awareness) have significantly reduced crime in other regions.
- Several task forces across the nation have taken a "community policing" approach toward cyber crime rating their successes not on traditional statistics such as arrests and convictions, but by the impact they have on the community.
- Computer networks owned and operated by New Hampshire government, heath care, and other vital industry systems are critical components of New Hampshire's infrastructure. Efforts to share information, understand vulnerabilities, and create teams of specialists to address future incidents may

increase the state's cyber security preparedness and is necessary for homeland security.

- The private sector owns and operates 80% of the nation's critical infrastructures and must be included as a critical partner in any plan to address cyber security preparedness statewide.
- Preparedness exercises to understand New Hampshire's cyber vulnerabilities may be a valuable tool in the future to address Homeland Security issues.

Immediate Goals

- 4.1 - To coordinate statewide cyber crime and homeland security efforts at all levels to avoid redundancy and make the most use of available resources.
- 4.2 - To establish a steering committee comprised of representatives of both industry and the public to ensure that the needs of New Hampshire's citizens are met.
- 4.3 - To develop and support public awareness programs through police departments by:
    a. Identifying and providing training materials at minimal costs to state and local agencies.
    b. Identifying other available resources to meet local efforts.
- 4.4 - To develop and deliver a public awareness campaign in order to increase the public's knowledge of the scope of computer related crimes.
- 4.5 - To hold annual statewide meetings for the benefit of the public to highlight criminal justice efforts, share information, and gather feedback from the citizens of New Hampshire.